UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/702,289	10/30/2000	Eva Chen	TRNDP004	1429

22434 7590 05/04/2005

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/702,289	CHEN ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/7/2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Amendment

Applicant's arguments/ amendments with respect to amended claims 1, 11, 12, and 22 and previously presented claims 2-10 and 13-21 filed December 7, 2004 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hailpern et al., United States Patent No. 6,275,937 and further in view of Trcka et al., United States Patent No. 6,453,345 and Tso et al., United States Patent No. 6,088,803.

As per claim 1:

Hailpern et al. substantially teach a real-time virus tracking and display system for use with a distributed computer network, the system comprising: a plurality of client users having potentially infected client computers (col. 7, lines 18-29); at least one anti-virus scanning server accessible via a network, whereby the client users contact the server to facilitate virus scanning of the client computers (col. 8 line 47 – col. 9 line 6, col. 11 lines 39-55, and col. 16 lines 25-37); and a database server associated with the virus-checking server for processing the scan log information into virus-tracking information (col. 9, lines 12-51).

Not explicitly disclosed by Hailpern et al. is the system wherein an anti-virus scanning server is accessible via the distributed computer network, a scan log which is sent back from each client user detailing certain results of the virus scanning on each client computer or a virus-tracking server for receiving the scan log information from said client computers in real-time. However Tso et al. teach that a system including a network could be modified in order for that system to work in a distributed network. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed in Hailpern et al. to implement the system in a distributed network. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Tso et al. in col. 8, lines 50-63.

Furthermore, Tso et al. teach that the results of the virus check are communicated and can be stored in cache that exists in a network device or in a device coupled to the network device. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed in Hailpern et al. to have the scan log communicated to the virus tracking server in real-time so that patterns of viruses can be monitored. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Tso et al. in col. 5, lines 1-43.

Also not explicitly disclosed by Hailpern et al. is at least one virus-tracking display mode accessible by a tracking user from the virus-tracking server, the display mode providing real-time updates of said virus-tracking information pertaining to the scan logs. However, Trcka et al. teach object class libraries for allowing the user to select between a variety of display formats,

including various graphs, lists, and tables for display of report data from analysis applications. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed in Hailpern et al. to have the collaborative server by displaying the occurrence of viruses so that an individual can easily recognize a viral threat to their computer system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Trcka et al. in col. 18, line 62 – col. 19, line 61.

As per claim 2:

Hailpern et al. fail to teach a tracking user from the virus-tracking server, the display mode provides real-time updates of virus information pertaining to the scan logs. Trcka et al. teach object class libraries for allowing the user to select between a variety of display formats, including various graphs, lists, and tables for display of report data from the analysis applications (col. 18, lines 62-66). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by providing for a display of the virus-tracking information in association with graphs, lists, and tables.

As per claim 3:

Hailpern et al. fail to teach display modes include a plurality of web pages with user selectable menus to configure the virus-tracking display on the pages. Trcka et al. teach displaying a surveillance data processing module enables authorized users to interactively analyze and manipulate traffic data through a powerful analysis tools. This includes displaying user specified types of network events, conducting pattern searches of selected packet data, reconstructing transaction sequences, and identifying predefined network problems (col. 13, lines

16-19). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by providing for web page selections to track specific viruses.

As per claim 4:

Hailpern et al. fail to teach a scan log contains no information relating to the direct identification of the client user. The automated monitor can be configured to generate a log file of specific types of events, such as unsuccessful logon attempts (col. 17, lines 37-43). However, no mention is made of the direct identification of the client user. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by preserving the privacy of the client user.

As per claim 5:

Hailpern et al. fail to teach that the scan log includes the name of the virus, the frequency of its occurrence, and the geographic location of the infected computer. Trcka et al. teach any of a variety of known security checks can be performed on the packet data at this stage. Virus checking can be performed on all incoming FTP and HTTP files from unknown sites (col. 14, lines 60-67 and col. 15, lines 1-4). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by presenting a tracking scan log with virus information of interest to a client user.

As per claim 6:

Hailpern et al. fail to teach a servlet program on the virus-tracking server is used to receive the scan log information from the at least one anti-virus scanning server. Trcka et al. teach the report generation module includes object class libraries for allowing the user to select

between a variety of display formats, including various graphs, lists, and tables for the display of report data from the analysis applications (col. 18, lines 62-67 and col. 19, lines 1-5. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing for the download of files to a program for anti-virus software.

As per claim 7:

Hailpern et al. fail to teach a polling program is used to regularly retrieve virus-tracking information from the database server and store it in a data object. Trcka et al. teach types of reports that can be generated using this application include the following: individual user activity; application activity; transaction activity; logons; and unauthorized access to restricted files and databases (col. 20, lines 13-17). These processes are used to track the viruses. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing for the polling of requested virus information and presenting it to the client user for installation of appropriate anti-virus programs in one's computers.

As per claim 8:

Hailpern et al. fail to teach a common gateway interface program used to retrieve the data object for display by the tracking user. Trcka et al. teach traffic capture components, which run continuously in the background, to passively generate a data stream that represents the traffic present on the network (col. 10, lines 60-66). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by reporting and logging information about viruses tracking for the client

user in order that the client may utilize the information to deploy anti-virus programs.

As per claim 9:

Hailpern et al. fail to teach a Java applet running on tracking user browser is used to display a real-time virus-tracing map. Trcka et al. teach three general types of software components run on the controller for the purpose of processing traffic data (col. 10, lines 59-60). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by adding a Java applet to decrease the CPU/modem time required to communicate with the server.

As per claim 10:

Hailpern et al. fail to teach the client user is also the tracking user. Trcka et al. teach from the screens, the user can specify such parameters as start time/date, end time/date, the types of events of interest. The user can specify search criteria and specific fields to be searched and can specify an output type of the display screen, the printer, or the file (col. 20, lines 5-12). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing the client user to also be the user, thus allowing individuals to set-up web sights and protect their computer from viruses by use of the allowed operations.

As per claim 11:

Hailpern et al., Trcka et al., and Tso et al. substantially teach the system as applied to claim 1 above. Furthermore, Tso et al. teach the system wherein the distributed computer network includes the Internet, wherein said scan log from each scanned client computer is sent back over the Internet to be received by said virus tracking server, and wherein said virus

tracking display mode is accessible over the Internet by said tracking user (col. 1, lines 18-55 and col. 2, lines 16-53).

As per claim 12:

Hailpern et al. substantially teach a method to provide real-time virus tracking and display for use with a distributed computer network, the method comprising: providing an anti-virus scanning program on at least one anti-virus scanning server accessible via a computer network (col. 8 line 47 – col. 9 line 6, col. 11 lines 39-55, and col. 16 lines 25-37); invoking the anti-virus scanning program from a plurality of client users having potentially infected client computers (col. 7, lines 18-29); and a database server associated with the virus-tracking server for processing the scan log information into virus-tracking information (col. 9, lines 12-51).

Not explicitly disclosed by Hailpern et al. is the method wherein an anti-virus scanning server is accessible via the distributed computer network, generating a scan log from each scanned client computer and sending the scan log back from each client user, the scan log detailing certain results of the scanning program on each client computer. However Tso et al. teach that a system including a network could be modified in order for that system to work in a distributed network. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hailpern et al. to implement the system in a distributed network. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Tso et al. in col. 8, lines 50-63.

Furthermore, Tso et al. teach that the results of the virus check are communicated and can be stored in cache that exists in a network device or in a device coupled to the network device.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hailpern et al. to have the scan log communicated to the virus tracking server in real-time so that patterns of viruses can be monitored. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Tso et al. in col. 5, lines 1-43.

Also not explicitly disclosed by Hailpern et al. is processing the scan log information into virus-tracking information and storing it on a database server associated with the virus-tracking server, and retrieving the virus-tracking information, and displaying a real-time trace on a tracking user device. However, Trcka et al. teach virus checking can be performed on all incoming FTP and HTTP files from unknown sites to analyze the data, it is passively capture. Furthermore, Trcka et al. teach the audit application presents the user with a set of display screens, which allow the user to specify various settings, and parameters for selectively viewing and generating audit trails from the archived traffic data. Finally, from these screens, the user can specify such parameters as start time/date, end time/date, and the type of events of interest.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hailpern et al. for allowing the collaborative server to track the virus information and store it so the analysis could be used to stop and prevent the virus from infecting computers. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Trcka et al. in col. 14 lines 62-67, col. 5 lines 1-4, and col. 20 lines 1-17.

As per claim 13:

Hailpern et al. fail to teach a tracking user from the virus-tracking server, the display mode provides real-time updates of virus information pertaining to the scan logs. Trcka et al. teach the Report Generation Module includes object class libraries for allowing the user to select between a variety of display formats, including various graphs, lists, and tables for the display of report data from the analysis applications (col. 18, lines 6266). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by providing for a display of the virus-tracking information in association with geographical locations.

As per claim 14:

Hailpern et al. fail to teach display modes include a plurality of web pages with user selectable menus to configure the virus-tracking display on the pages. Trcka et al. teach the Surveillance Data Processing Module is to enable authorized users to interactively analyze and manipulate pre-recorded traffic data through a set of powerful analysis tools (col. 13, lines 16-19). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by providing for web page selections to track specific viruses.

As per claim 15:

Hailpern et al. fail to teach a scan log contains no information relating to the direct identification of the client user. Trcka et al. teach the generation of a log file of specific events, such as unsuccessful logon attempts (col. 17, lines 37-43). No information about direct identification of the client user is mentioned. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s

collaborative server by preserving the privacy of the client user.

As per claim 16:

Hailpern et al. fail to teach that the scan log includes the name of the virus, the frequency of its occurrence, and the geographic location of the infected computer. Trcka et al. teach the report generation module includes Report Generation Module includes object class libraries for allowing the user to select between a variety of display formats, including various graphs, list, and tables for the display of report data from the analysis applications (col. 18, lines 62-66). These display formats are suited for the presentation of the name of the virus, frequency of occurrence, and geographical location. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by presenting a tracking scan log with virus information of interest to a client user.

As per claim 17:

Hailpern et al. fail to teach a servlet program on the virus-tracking server is used to receive the scan-log information from the at least one anti-virus scanning server. Trcka et al. teach the report generation module includes object class libraries for allowing the user to select between a variety of display formats, including various graphs, lists, and tables for the display of report data from the analysis applications (col. 18, lines 62-67 and col. 19, lines 1-5). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing for the download of files to a program for anti-virus software.

As per claim 18:

Hailpern et al. fail to teach a polling program is used to regularly retrieve virus-tracking

information from the database server and store it in a data object. Trcka et al. teach examples of the types of reports that can be generated using this application include the following: individual user activity, application activity, socket activity, transaction activity, logons, and unauthorized accesses (col. 20, lines 13-17). This generation process may retrieve virus information and store it for later access. It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing for the polling of requested virus information and presenting it to the client user for installation of appropriate anti-virus programs in one's computers.

As per claim 19:

Hailpern et al. fail to teach a common gateway interface program used to retrieve the data object for display by the tracking user. Trcka et al. teach traffic capture components, which run continuously in the background, to passively generate a data stream that represents the traffic present on the network (col. 10, lines 60-66). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by reporting and logging information about viruses tracking for the client user in order that the client may utilize the information to deploy anti-virus programs.

As per claim 20:

Hailpern et al. fail to teach a Java applet running on tracking user browser is used to display a real-time virus-tracing map. Trcka et al. teach three general types of software components run on the controller for the purpose of processing traffic data (col. 10, lines 59-60). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by adding a Java applet to

decrease the CPU/modem time required to communicate with the server.

As per claim 21:

Hailpern et al. fail to teach the client user is also the tracking user. Trcka et al. teach from the screens, the user can specify such parameters as start time/date, end time/date, the types of events of interest. The user can specify search criteria and specific fields to be searched and can specify an output type of the display screen, the printer, or the file (col. 20, lines 5-12). It would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Hailpern et al.'s collaborative server by allowing the client user to also be the user, thus allowing individuals to set-up web sights and protect their computer from viruses by use of the Tracking Center.

As per claim 22:

Hailpern et al., Trcka et al., and Tso et al. substantially teach the system as applied to claim 12 above. Furthermore, Tso et al. teach the method wherein the distributed computer network includes the Internet wherein said scan log from each scanned client computer is sent back over the Internet to be received by said virus tracking server, and wherein said real-time trace displayed on said tracking user device is made available over the Internet (col. 1, lines 18-55 and col. 2, lines 16-53).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi

Nadia Khoshnoodi
Examiner
Art Unit 2133
4/27/2005

NK

GUY LAMARRE
PRIMARY EXAMINER